

Thoughts on Privacy

concepts and approaches

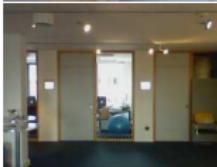
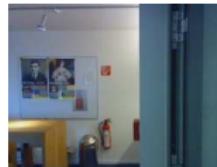
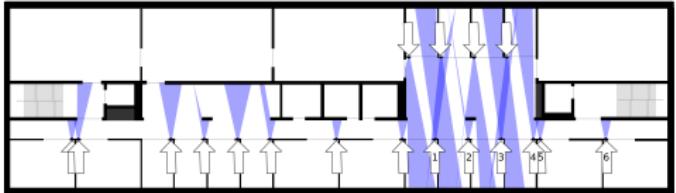
Dr. Jasper van de Ven

24th May 2018

motivation

it's law... obey it

my motivation



ethics & privacy

Ethics

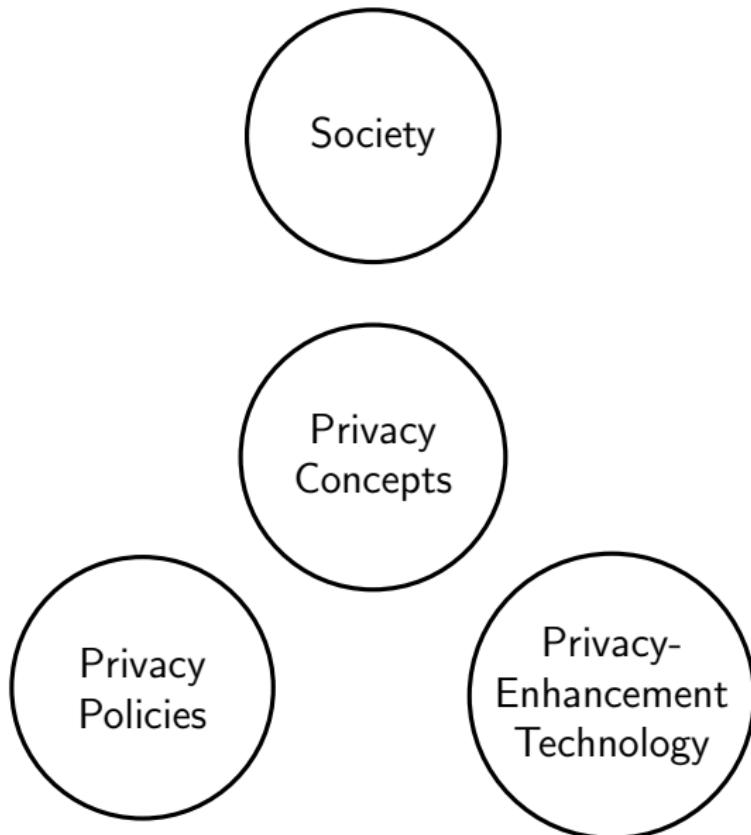
Ethics is the concept of right and wrong, determining what is right and wrong.

(images are from google image search thumbnails)



The image is a word cloud centered around the Facebook logo. The words are in various sizes and colors, including shades of blue, red, and black. The most prominent words include 'CAMPAIGN', 'RELATIVES', 'KOGAN', 'MERCERS', 'MESSANGER', 'BANNON', 'TRUMP', 'PRIVACY', 'FRIENDS', 'APP'S', 'VIDEOS', 'ONLINE', 'SMS', 'PICTURES', 'FRIENDS', 'CAMBRIDGE ANALYTICA', 'FOREIGN WORKERS', 'EMBEDDED', 'WYLIE', 'POSTS', 'ACCESS', 'NIX', 'TIMID', 'KUSHNER', 'EXTERVOTS', 'ZUCKERBERG', 'BUSINESS', 'CRAZU', 'DATA', 'PARSCALE', 'CONNECTIONS', 'ADVERTISING', 'SECURITY', 'PROFILE', 'WALL', 'QUIZ', 'WHISTLE-BLOWER', 'THIS IS YOUR DIGITAL LIFE', 'DATA-HARVESTING', 'MTURK', 'QUALTRICS', and 'SOCIAL MEDIA INTERNET'.

privacy overview



society



CONSTITUTION **NATIONS** **PRESIDENT** **DEMOCRACY** **FEDERAL** **VOTERS** **DIPLOMACY** **REPRESENTATIVE** **VALUES** **TACTICS** **RIGHT**
HYPOCRISY **POLITICS** **PARTIES** **FOREIGN** **POLLS** **REGULATIONS** **MONARCH**
REGULATION **INSTITUTIONS** **GOVERNMENT** **ADMINISTRATION** **STATE**
FAIRNESS **ACTION** **DECENCY** **LEFT** **REVOLUTION** **CONTROL** **HONOR** **CAMPAIN** **MONETARY** **SOCIALISM**
CAPITALIST **VIRTUE** **STANDARDS** **TACTICS** **CIVILIAN** **LEGISLATURE** **CITIZENS** **POLICY**
UNION **CORRUPTION** **DICTATOR**

(images are from google image search thumbnails)

privacy concepts

- Information Privacy
- Personal Privacy
- Territorial Privacy
- Location Privacy

privacy concepts

- Information Privacy ←
- Personal Privacy
- Territorial Privacy
- Location Privacy

accessibility and availability of information, including but not limited to personally identifiable information (PII) and sensitive personal information (SPI)

privacy concepts

- Information Privacy
- Personal Privacy ←
- Territorial Privacy
- Location Privacy

follows the concept of information privacy with a focus on personally identifiable information (PII) and sensitive personal information (SPI)

privacy concepts

- Information Privacy
- Personal Privacy
- Territorial Privacy ←
- Location Privacy

privacy as a spatial
and temporal problem

privacy concepts

- Information Privacy
- Personal Privacy
- Territorial Privacy
- Location Privacy ←

explicitly addresses location information, i.e., information about the (current) location of an individual or entity

privacy policy languages

LANGUAGE	FOCUS	machine	human	privacy	security	authorization context	meta	spatial	temporal	user	enterprise	multi-party	law	XML/RDF	high-level	logical	specific
...																	
P3P (1999)	✓	✓				✓	✓	○ ^a					✓ ^b		✓		
CPEExchange (2000)			✓			✓			✓						✓		
APPEL (P3P) (2001)	✓		✓			✓	✓			✓					✓		
E-P3P (2002)	✓		✓			✓	✓					✓			✓		
EPAL (2003)	✓		✓			✓	✓					✓			✓		
XPref (2005)	✓		✓			✓	✓					✓			✓		
LPU/CI (2006)	○		✓			✓	✓			✓			✓			✓	
Privacy APIs (2006)	✓		✓			✓	✓					✓	✓		○	○	✓
P-RBAC (2007)	✓	○	✓			✓	✓			✓	✓				✓		
PPL (2009)	✓		✓			✓	✓		✓			✓			✓		
SecPAL4P (2009)	✓	○	✓			✓	✓		✓			✓			✓		
PrivacyLFP (2010)	○		✓			✓	✓			✓			✓		✓		
AIR (2010)	✓		✓				○ ^h							✓ ^f		○ ^g	
S4P (2010)			✓						✓			✓			✓		
Jeeves (2012)	○		✓			✓						✓		✓		✓	
P2U (2014)	✓		✓			✓	✓		✓ ^e	✓				✓		○ ⁱ	
AAL/A-PPL (2014)	✓	✓	✓	○		✓	✓		✓	✓		✓					✓
...																	

29 Languages focusing on privacy and security policies from 1999 till 2014

privacy policy languages

LANGUAGE	machine	human	privacy	security	authorization	context	meta	spatial	temporal	user	enterprise	multi-party	law	XML/RDF	high-level	logical	specific
	FOCUS							ASPECTS						SYNTAX			
...																	
P3P (1999)	✓	✓			✓	✓		○ ^a					✓ ^b	✓			
CPEExchange (2000)		✓	✓		✓	✓			✓					✓	✓		
APPEL (P3P) (2001)	✓	✓			✓	✓				✓				✓	✓		
E-P3P (2002)	✓	✓			✓	✓					✓			✓	✓		
EPAL (2003)	✓	✓			✓	✓					✓			✓	✓		
XPref (2005)	✓	✓			✓	✓					✓			✓	✓		
LPU/CI (2006)	○	✓			✓	✓			✓				✓	✓	○	✓	
Privacy APIs (2006)	✓	✓			✓	✓							✓	○	○	✓	
P-RBAC (2007)	✓	○	✓		✓	✓				✓	✓			✓			
PPL (2009)	✓	✓			✓	✓			✓ ^a	✓			✓	✓	✓		
SecPAL4P (2009)	✓	○	✓		✓	✓				✓			✓	✓	✓	✓	
PrivacyLFP (2010)	○	✓			✓	✓				✓			✓	✓	✓	✓	
AIR (2010)	✓	✓				○ ^h							✓ ^f	○ ^g			
S4P (2010)		✓							✓						✓		
Jeeves (2012)	○	✓			✓								✓	✓	✓	✓	
P2U (2014)	✓	✓			✓	✓			✓ ^e	✓			✓				
AAL/A-PPL (2014)	✓	✓	✓	○	✓	✓		✓	✓				✓	○ ^l			✓
...																	

29 Languages focusing on privacy and security policies from 1999 till 2014

machine	22
human	5
privacy	18
security	12
authorization	26
context	16
meta	1
spatial	9
temporal	10
user	4
enterprise	11
multi-party	8
law	3
XML/RDF	19
high-level	6
logical	11
specific	7

privacy enhancing technology

- authentication
- accountability
- encryption
- obfuscation
- fragmentation
- data-hiding
- social means

privacy enhancing technology

- authentication ←
- accountability
- encryption
- obfuscation
- fragmentation
- data-hiding
- social means

methods to validate and enforce a users authentication and authorization to access certain information

privacy enhancing technology

- authentication
- accountability ←
- encryption
- obfuscation
- fragmentation
- data-hiding
- social means

allow to relate actions or information to specific entities

privacy enhancing technology

- authentication
- accountability
- encryption ← methods to encrypt and
● obfuscation decrypt information
- fragmentation
- data-hiding
- social means

privacy enhancing technology

- authentication
- accountability
- encryption
- obfuscation ←
- fragmentation
- data-hiding
- social means

possibilities to prevent the complete disclosure of detailed information, but allows to present or access abstracted versions

privacy enhancing technology

- authentication
- accountability
- encryption
- obfuscation
- fragmentation ←
- data-hiding
- social means

methods to distribute information in order to dissolve sensitive relational information

privacy enhancing technology

- authentication
- accountability
- encryption
- obfuscation
- fragmentation
- data-hiding ←
- social means

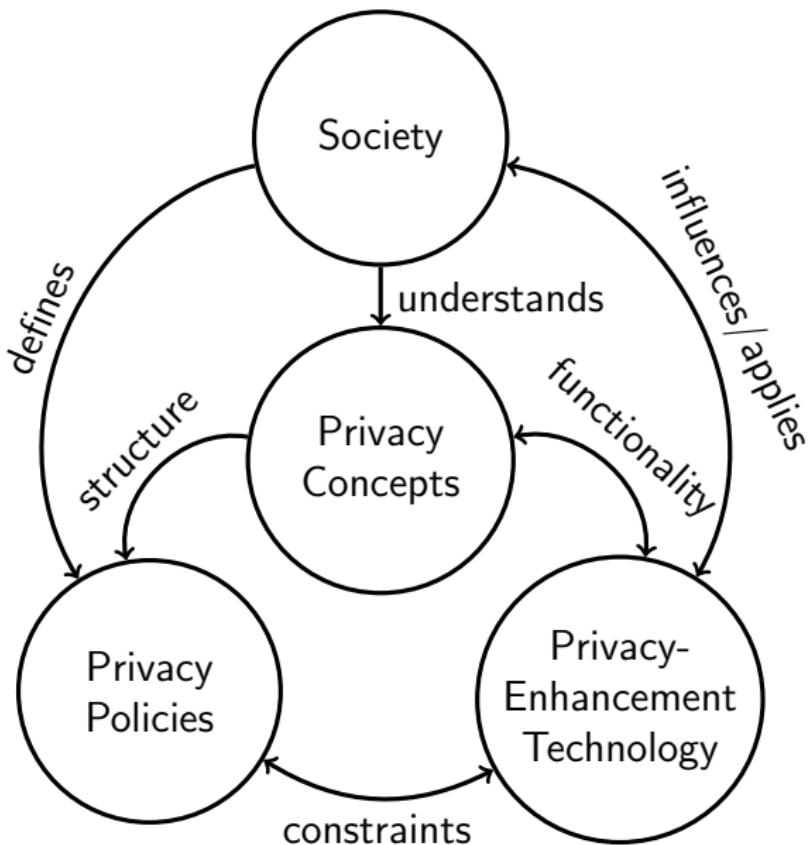
methods to prevent
the availability or visibility
of information

privacy enhancing technology

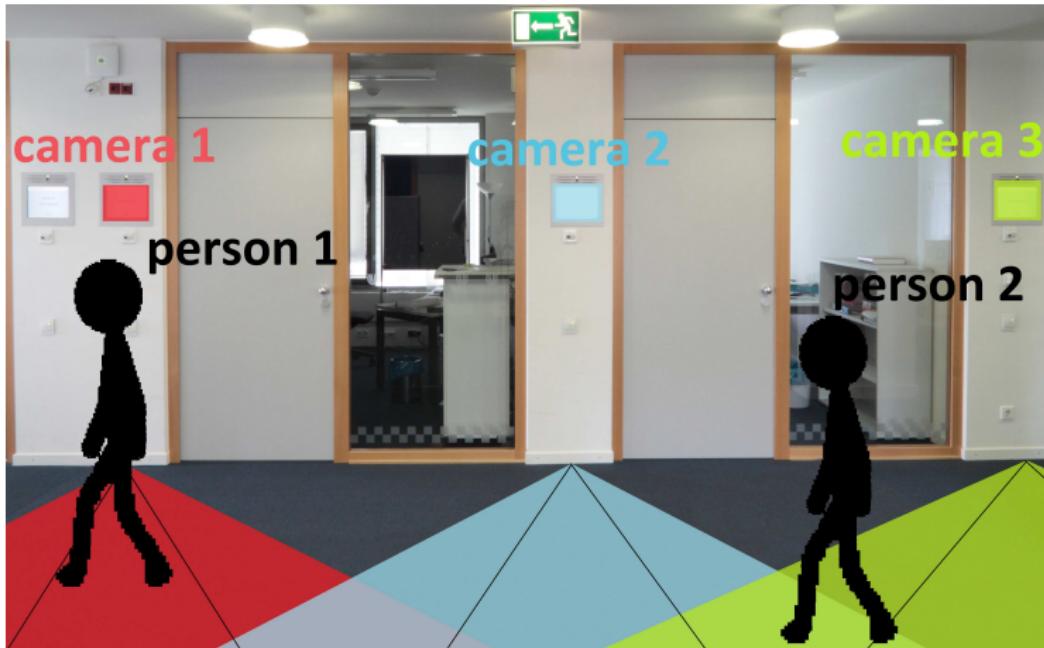
- authentication
- accountability
- encryption
- obfuscation
- fragmentation
- data-hiding
- social means ←

methods applied by a society to restrict and enforce actions conducted by other individuals or groups

privacy overview



privacy paradox



privacy as a service

knowledge vs support



- transparency
- responsibility
- privacy (violation) disclosure

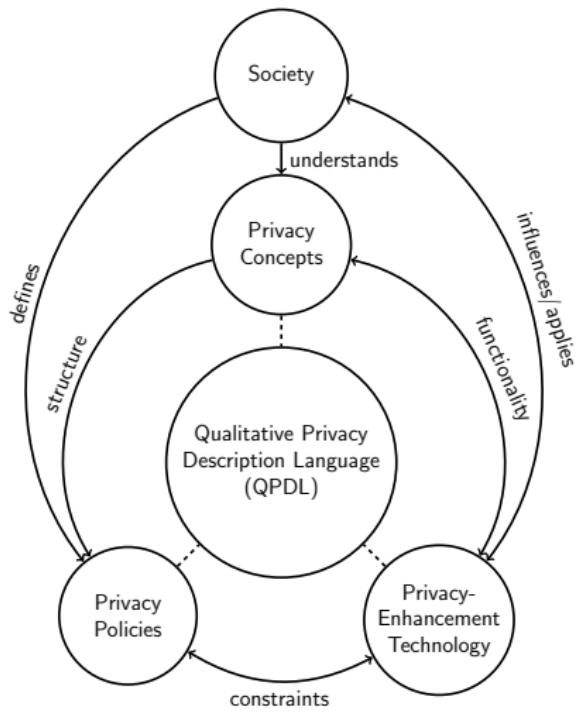
privacy affordances

how to deal with privacy violations in a system?

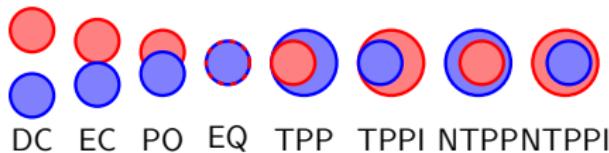
	detection	resolution	prediction	prevention
privacy oblivious systems				
privacy aware systems	✓			
privacy repairing systems	(✓)	✓		
privacy projecting systems	(✓)		✓	
privacy conserving systems	(✓)	✓	✓	
privacy shielding systems	(✓)	(✓)	(✓)	✓

(-) Implied by other privacy functionality used or possible, but without impact

QPDL



QSTR



temporal logics (LTL/ATL)

- | | |
|----------------|--------------|
| $\circ\phi$ | (next) |
| $\Box\phi$ | (always) |
| $\Diamond\phi$ | (eventually) |
| $\phi U \psi$ | (until) |
| $\phi R \psi$ | (release) |

QPDL

- spatial symbols (\mathcal{S})
- qualitative relation symbols (\mathcal{R})
- function symbols (\mathcal{F})
- general propositional symbols (\mathcal{G})

$$P := G \cup \{r(s, t) | r \in \mathcal{R}, s, t \in (\mathcal{S} \cup \{f(s_i) | f \in \mathcal{F}, s_i \in \mathcal{S}\})\}$$

QPDL

$$\Pi := \bigcup_{i=1,\dots,m} \pi_i$$

$$\pi_i = \{\phi_{i_1}, \phi_{i_2}, \dots, \phi_{i_o}\}$$

$$\phi_{i_j} \rightarrow violated(\phi_{i_j})$$

$$violated(\pi_i) := \bigvee_{j=1,\dots,l} violated(\phi_{i_j})$$

$$violated(\Pi) := \bigvee_{i=1,\dots,m} violated(\pi_i)$$

QPDL

- $(knows(h_2, name(h_1)) \implies \neg knows(h_2, address(h_1))) \wedge (knows(h_2, address(h_1)) \implies \neg knows(h_2, name(h_1)))$
- $(knows(h_2, name(h_1)) \wedge knows(h_2, address(h_1))) \implies (in(h_1, r) \wedge in(h_2, r))$
- $stored(data) \wedge encrypted(data)$
- $\neg access(h, data) \vee valid_code(h)$
- $(in(h_1, r) \wedge in(h_2, r)) \implies \circ(show(data, t) \wedge in(t, r))$

privacy vs security

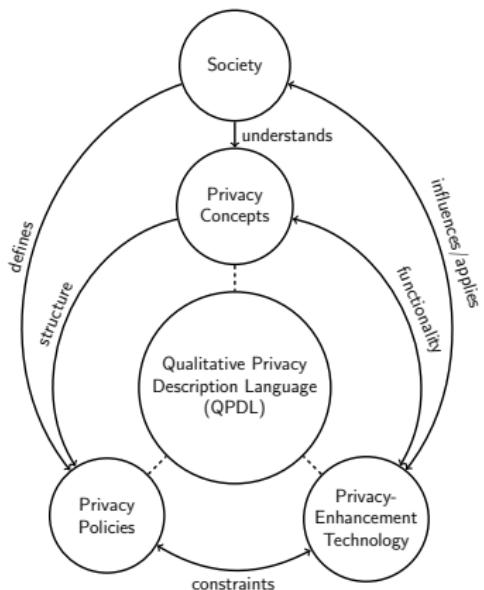
privacy

- data avoidance/thrift
- intention of use
- duration of existence

security

- authenticity
- integrity
- confidentiality
- availability
- non repudiation

summary



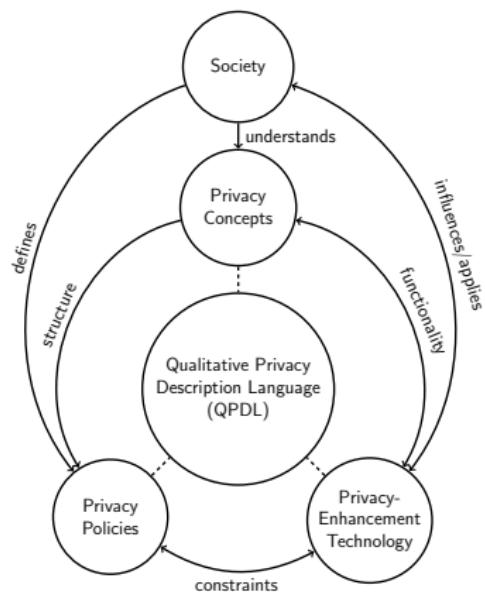
- concepts
- policy languages
- technologies
- paradoxes
- privacy as a service
- privacy vs security

take home messages

- privacy is important
- balance knowledge and support
- privacy is an opportunity
- privacy is a socio-technical problem

thank you!

- questions?
- comments?



vandeven@uni-bremen.de

<https://cosy.informatik.uni-bremen.de/staff/jasper-van-de-ven.html>

https://www.researchgate.net/profile/Jasper_Van_De_Ven